「医療情報システムの安全管理に関するガイドライン　第 5.2 版」に関するＱ＆Ａ

令和４年〇月

総論

Q－１
① このガイドラインを遵守すべき対象者は誰か。
② このガイドラインはシステムベンダに読んでもらえば、医療機関等の関係者まで読む必要はないのではないか。
③ 再委託する場合の再委託先事業者もこのガイドラインを遵守することとなるのか。また、他に遵守すべきガイドラインがあるのか。

Ａ
① 医療情報システムを運用する医療機関等の組織の責任者の方です。
② 医療情報システムの管理上の一次責任は医療機関側にあります。安全管理は運用と技術とが相まって一定のレベルを達成するものです。このガイドラインに則った、実際のシステム構築の多くはシステムベンダが行うかもしれません。しかし、それを管理・運用するのは、あくまで医療機関側の責任です。医療機関等の関係者は、このガイドラインの内容をよく理解し、遵守していただく必要があります。
③ 再委託先でもこのガイドラインが遵守されるよう、指導・監督していただく必要があります。医療情報システムの安全管理の観点ではこのガイドラインを、医療情報システムで取り扱う個人情報の保護の観点では「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」を遵守することが必要です。医療情報システム・サービスの提供事業者向けには、総務省・経済産業省が「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」を発行しており、こちらも参考にする必要があります。

Q－２ 「医療情報システム」とは具体的に何を示すのか。

Ａ 医療機関等のレセプト作成用コンピュータ（レセコン）、電子カルテ、オーダリングシステム等の医療事務や診療を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するようなコンピュータや携帯端末も範ちゅうとして想定しています。また、患者情報が通信される院内・院外ネットワークも含まれます。

Q－３
① このガイドラインの対象情報の範囲はどこまでか。
② 他の医療機関等から提供された電子化された情報の取扱いは、このガイドラインの対象となるのか。

Ａ このガイドラインは、医療に関わる情報を扱う全ての情報システムと、それらのシステムの導入、運用、利用、保守及び廃棄に関わる人又は組織が対象となっています。

そのため、このガイドラインの対象情報は、前文の情報システムや人又は組織の中で扱われる情報のうち、①「「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」の一部改正について」（平成 28 年３月 31 日付け医政発 0331 第 30 号・薬生発 0331 第 10 号・保発 0331 第 26 号・政社発 0331 第１号厚生労働省医政局長・医薬・生活衛生局長・保険局長・政策統括官（社会保障担当）連名通知。以下「施行通知」という。）に含まれている文書、②施行通知には含まれていないものの、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成 16 年法律第 149 号。以下「e-文書法」という。）の対象範囲で、かつ、患者の医療情報が含まれている文書等（麻薬帳簿等）、③法定保存年限を経過した文書等、④診療の都度、診療録等に記載するために参考にした超音波画像等の生理学的検査の記録や画像、⑤診療報酬の算定上必要とされる各種文書（薬局における薬剤服用歴の記録等）等が対象です。

したがって、他の医療機関から提供された電子化された情報についても、電子化された状態で利用・保存する限りはこのガイドラインの対象となります。

なお、個人情報の取扱いについては、個人情報の保護に関する法律（平成１５年法律第５７号。以下「個人情報保護法」という。）並びに「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」等を参照してください。

Q－４ 医療情報の取扱いに際し、医療機関等にはどのような責任が生じることになるか。

Ａ 患者情報の取扱いにおいては、まず医師法、医療法等において適正な管理が

求められており、例えば医療法では診療記録を適切に備えることが求められています（第 21 条第１項第９号等）。

また医療情報は患者に関する個人情報であることから、個人情報保護法の適用対象になることは言うまでもありません。令和２年改正個人情報保護法では個人情報取扱事業者（医療機関等も含む）が医療情報のような要配慮個人情報を流出させた場合には、個人情報保護委員会に報告し、本人にも通知することが義務づけられました（法第 26 条、規則第６条の２、第６条の３）。

そのような報告義務・通知義務や、その前提である個人情報の安全管理のために措置を講じる義務（法第 23 条）等に違反しており、個人の権利利益を保護するため必要があると認められた場合には、個人情報保護委員会から当該医療機関等に対して是正勧告がなされることになります（法第 145 条第１項）。さらに是正勧告に正当な理由なく対応しない、違反行為がなされる等により、個人の重大な権利利益の侵害が切迫していると認められた場合には、個人情報保護委員会から違反行為の中止や是正措置実施の命令がなされます。（法第 145 条第２項、第３項）

令和 2 年改正個人情報保護法では、個人情報保護法に対する重大な違反行為に対する罰則も強化されています。例えば、上記の個人情報保護委員会から医療機関等に対する命令違反が生じた場合、命令違反をした場合の代表者や従業員が属する法人に対する罰金刑は従来の 30 万円以下から 1 億円以下に大きく強化されています。医療情報などの個人情報データベースを、不正に提供等を行った場合も同様の罰金刑となっています（法 179 条第１項）。

このように個人情報保護法では医療情報が漏洩した場合の報告義務等や、これに関連して必要な対応を行わずに命令違反を行った場合の医療機関等に対する罰則などが強化されていることを十分理解する必要があります。

Q－５　どのような場合に、介護事業者は本ガイドラインの内容を遵守する必要があるか。

Ａ　本編 3.1 章を踏まえて、下記のような事例等が想定されます。

- 介護事業者が取り扱う e-文書法の対象範囲となる文書に、医師等から提供を受けた患者の医療情報を記入し、電子保存を行う場合。別冊 3.1 章に、医療情報が含まれることがある介護事業者の文書が例示されているため、ご参照ください。
- 上記のほか、医師等が作成した患者の医療情報を情報システムにより取

り扱う場合。

Q－6　SNS で患者情報をやり取りする場合、ガイドライン上講じるべき対策はあるか。

A　SNS（Social Networking Service）において患者の医療情報を取り扱う場合、当該サービスは医療情報システムに該当し、ガイドラインの基準を満たす必要があります。

SNS には、セキュリティが十分に確保されていないサービスもあることから、一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）が公表している「医療情報連携において、SNS を利用する際に気を付けるべき事項」[1]を参考に、適切な対策を講じてください。

Q－7　このガイドラインに従いシステム構築をしていたにも関わらず起こった事故について、責任のあり方をどのように考えるべきか。

A　このガイドラインは、医療情報システムの安全管理及び e-文書法への適切な対応に関し、厚生労働大臣が法を執行する際の基準となるもののーつです。技術的なことだけではなく、運用を含めた安全対策を示したものであり、ガイドラインを遵守していたと認められる状況下で起こった事故については、一定の法的責任を果たしていたということが可能だと考えられます。

しかしながら、その事故によって患者等の第三者が不利益を被った場合に全て免責されない可能性もあります。医療情報システム運用時の責任についての考え方が第４章に記述されているため、ご参照下さい。

Q－8
① 旧版のガイドラインも全て読む必要があるか。
② 技術の進歩は著しいが、このガイドラインは定期的に見直されるのか。
③ 別冊も全て読む必要があるか。

A
① 旧版は読む必要はありません。旧版の内容は、最新版で変更若しくは削

[1] http://www.hispro.or.jp/open/pdf/SNS_RiyouCheckJikou_20160126.pdf

除等されている場合があるため、最新版をお読みください。
② このガイドラインは適宜見直すこととしております。
③ ガイドラインの本編において、医療機関等において実施すべき内容を示し、別冊でその考え方や、具体的な対応例などを示しています。具体的な対策を検討するに際して、本編で述べた内容の考え方や具体例などを確認するために、できるだけ別冊についてもお読みください。

Q－９
① 「C.最低限のガイドライン」さえ措置すればよいのか。
② 「C.最低限のガイドライン」は守っていたが、「D.推奨されるガイドライン」を守っていなかったために、裁判で不利になることはないか。

A
① 各項目での「C.最低限のガイドライン」は、制度上の要求を満たすための文字どおり「最低限」実施すべき事項です。施設の規模や体制によって要求される事項は異なるため、「D.推奨されるガイドライン」を考慮し、最適の対策を行う必要があります。
② このガイドラインは医療情報システムの安全管理及び e-文書法への適切な対応のため、所要の対策を示したガイドラインであり、それ以外の民事訴訟、刑事訴訟に対して「D.推奨されるガイドライン」を遵守しているかどうかは、直接的な判断基準にならないと考えます。裁判に至る個々の事例により事情は異なるため、不利になるかどうかについては一概にいえません。「D.推奨されるガイドライン」の採否については、医療機関等の方針に基づいて適切に判断し、運用してください。

Q－１０
① このガイドラインに違反した場合の罰則等はあるのか。
② ガイドラインを遵守しなかった場合、e-文書法以外に抵触する法令はあるのか。
③ ガイドラインの「C.最低限のガイドライン」を実施しなかった場合、具体的な罰則規定があるのか。

A 本ガイドラインは、e-文書法が医療分野において執行される際の指針となります。
ガイドライン自体に罰則はありませんが、ガイドラインに違背した状態

は、法令を遵守していないとみなされる可能性が十分にあります。
　ガイドラインの「C.最低限のガイドライン」には、法令により要求されている事項等が列挙されています。したがって、これに違背することにより、e-文書法に求められる要件を満たすことができていないと認められる場合には、医療に関係する多くの法令等に違反したとみなされ、その罰則が適用されるおそれがあります。

Q－１１　診療所においても、大規模な医療機関と同じような対策が必要なのか。

Ａ　制度上の要求事項は同一ですので、規模に関わらず制度上の要求事項を満たす必要がありますが、具体的な対策については、医療機関等の規模に応じて対策のレベルが変わることがあります。例えば、医師１名のみで運営している診療所においてはシステムの利用者は１名になるため、「6.5　技術的安全対策」において利用者の識別・認証における技術的対策として求められている「C.最低限のガイドライン　6.」の医療従事者や関係職種のレベルに沿ったアクセス管理は事実上不要になります。具体的な対策の要否や対策レベルについては、医療機関等の規模や物理的な構造、運用形態によりで適切な対策が異なるため、各章の本編の「B.考え方」、および別冊の各章を参考にご検討ください。

Q－１２　このガイドラインの説明会や研修会等は実施されていないのか。

Ａ　厚生労働省として実施しているものはありませんが、一般社団法人日本医療情報学会や一般社団法人保健医療福祉情報システム工業会等による講演会等で、解説が行われることがあります。
　なお厚生労働省では、医療機関等向けサイバーセキュリティ研修用動画、教材を提供しております[2]ので、こちらも参考にしてください。

[2] https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

「3　本ガイドラインの対象システム及び対象情報」関係

Q－１３　電子保存が認められている文書とは具体的に何か。

Ａ　「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」（平成 17 年厚生労働省令第 44 号。以下「e-文書法省令」という。）、施行通知で定められた文書で、具体的には別冊「3.1 第７章及び第９章の対象となる文書についての解説」に列挙されたものです。

「4　電子的な医療情報を扱う際の責任のあり方」関係

Q－１４　情報等の漏えい事故があった場合には、受託する事業者に対応をさせればよいのか。

Ａ　漏えい等の事故に際しては、当該情報を一次管理している医療機関等側に、説明責任、及び善後策を講ずる責任が発生します。もちろん事故を起こした事業者側も責任を免れるものではなく、両者が協力して説明及び善後策を講じる必要があります。

Q－１５　通常運用における説明責任を果たす際に、患者に説明すべき範囲はどこまでか。

Ａ　「診療情報を適正に保存するとともに、適正に利用すること」を医療情報システムの安全管理に関する方針の中に盛り込み公表する必要があります。また、詳細は、苦情・質問を受け付ける窓口を設け、「４.１　医療機関等の管理者の情報保護責任について（１）①」の項目の問い合わせに回答できるように、準備しておく必要があります。

Q－１６

① 請負事業者との対応にあたる「個人情報保護の責任者」になる要件はあるのか。

② 「個人情報の保護について一定の知識」とは何か。

Ａ

① 具体的な要件が定められているものではありませんが、医療に関わる全ての行為は、医療法等で医療機関等の管理者の責任で行うことが求められています。そのため、結果的には、個々の医療機関等の管理者が、権限を一部委譲するに適当と考える者を「個人情報保護の責任者」として選任することになると考えられます。

② 「電子化された個人情報の保護についての一定の知識」についても、具体的な条件は示されていません。電子化された情報は、紙媒体の情報に比べ容易に大量の情報が漏洩する可能性がある特徴を持つことから、それらの特徴と扱い方について理解していることが重要です。

Ｑ－１７　委託と第三者提供の情報管理責任上の違いは何か。

Ａ　委託とは、契約書等に基づき、業務の一部（例えば臨床検査）を外部に託すものであり、その情報の管理責任は一義的には委託元にあります。したがって、委託元は委託先の情報管理を監督しなければなりません。

それに対し、第三者提供（例えば紹介状による治療情報の提供）とは、患者等の同意の下に情報を他の事業者等に提供することです。第三者提供では、情報提供が確実に行われた時点で提供された情報の管理責任は提供先に移動します。

ただし、電子化情報は提供が行われた場合でも提供元にも同じ情報が残ることが多く、残った情報の管理責任がなくなるわけではありません。

Ｑ－１８　第三者提供が成立する時点はいつか。

Ａ　第三者提供は、原則本人の同意の下に情報が第三者に移動し、説明責任を含む管理責任が第三者に生じることを指します。

第三者が明確に自己の管理範囲に情報が存在することを確認した時点が、第三者提供の成立した時点になります。したがって、何らかの方法で受領確認を行う必要があり、受領確認がなされた時点と考えることができます。

オンラインで情報を送付する場合も同様であり、例えば相手のデータベースに格納されたことを電子的に確認する手続きを明確にした上で、その確認

をもって第三者提供が成立することを、契約等で合意することが必要です。送り手は送付したと考えているものの、受け手が受領したと認識していない等、責任の空白ができないようにする必要があります。

「5　情報の相互運用性と標準化について」関係

Q－１９　「５　情報の相互運用性と標準化について」は具体的に何を遵守すればよいのか。

Ａ　「５　情報の相互運用性と標準化について」では、相互運用性の重要性と、それを実現するために医療機関等がシステムベンダに要求すべき内容が記述されています。具体的には、医療機関等はシステムベンダの標準化に対する基本スタンス、（標準に対応していないならば、その理由や対応案）についてシステムベンダから説明を受け、一定の理解を等しくしておくことが求められます。さらに、現在導入しているシステムの更新やシステムの新規導入の際に、システム間でのデータ互換性やシステム接続性が確保されるように、医療機関等においても相互運用性に係る中長期的なビジョンを持ち、計画的にベンダへ要求していくことが望まれます。

Q－２０
① 相互運用性と標準化を行うことのメリットは何か。
② 基本データセットや標準的な用語集、コードセットを実装しなかった場合、どのような不利益が想像されるか。

Ａ
① 標準化のメリットには、システム間の相互運用性、データの長期的可用性等の確保があります。患者紹介や地域連携等で外部の医療機関等と診療情報をやり取りする場合、使用されているコードや用語が標準的でないと、適切な情報交換が難しくなります。また、システムをリプレイスする場合も、データ変換等が必要になってしまいます。
　これらの場合に、コードや用語が標準化されていれば、データ変換の手間や、変換機能の実装に必要な費用と時間の節約が期待できます。
② システム更新時のデータ移行に伴う作業によって、見読性、真正性の責任が果たせなくなることがあります。

Q－２１　基本データセットを利用し、一般財団法人医療情報システム開発センター（MEDIS-DC）の標準マスタを組み合わせた場合、医療情報システムのリプレイス時の相互運用性は保証されるか。

Ａ　基本データセット及び標準マスタを活用することは、相互運用性の確保を容易にしますが、保証はされません。なお、基本データセットに含まれない項目や標準が定められていない用語・コードも存在します。

　基本データセットや標準マスタは、概ね重要あるいは実装頻度の高いものを対象にしており、採用することによって、相互運用性を確保するためのコストを大幅に下げることができます。

Q－２２　外字の使用について注意すべき点は何か。

Ａ　外字を使用したシステムでは、あらかじめ使用した外字のリストを管理しておき、システムを変更した場合又は他のシステムと情報を交換する場合に、表記に齟齬のないよう対策する必要があります。

「6　医療情報システムの基本的な安全管理」関係

Q－２３　医療情報を電子化するに当たって定められた要件は何か。

Ａ　電子化する対象である全ての記録に対しての指針が、「６　医療情報システムの基本的な安全管理」に記載されています。さらに、保存義務のある記録の電子化には、e-文書法省令に従った内容が「７　電子保存の要求事項について」に記載されており、いわゆる電子保存の３要件（真正性、見読性、保存性）について規定されています。紙媒体の原本をスキャナで読み取り電子文書化する場合の記載は、「９　診療録等をスキャナ等により電子化して保存する場合について」に記載されています。保存義務のない書類であっても、これらの記載に準拠することが求められます。

Q－２４　不正ソフトウェア対策等が大変なので、外部と遮断した環境を設定する方が望ましいのか。

Ａ　医療情報の有効な利用を図るために、外部との接続を行うことも広く行われるようになっています。このような環境での不正ソフトウェア混入等の脅威は確かにありますが、効果的な対策を行うことで、リスクを許容範囲に収めることが可能です。また、外部と遮断することによって、不正ソフトウェア混入のリスクを低減できることは事実ですが、それだけで侵入を完全に防ぐことはできません。例えば、従業者が不用意に USB ポートなどを利用する場合等でも、不正ソフトウェアが混入することがあります。よって、外部と遮断されている環境であっても、不正ソフトウェア対策ソフトの導入、ぜい弱性の対策を行ったソフトウェアの利用等の対策が必要です。

なお、不正ソフトウェア対策ソフトやぜい弱性の対策等については、外部との接続を断つことによって、最新のソフトウェア検知パターンファイルの取得、対策ソフトウェアの緊急アップデート等を、可搬記憶媒体を介して手作業により行うことになるため、作業が遅れたり、可搬記憶媒体が不正ソフトウェアの混入源となったりするリスクがあります。一方で、外部との接続を遮断しつつ、管理者が安全な形で外部から取得した最新の内部サーバから配信するという手段もありますので、利便性とリスクを踏まえて対応することになります。

また端末やサーバ装置の活動を監視し、不正プログラム等の検知や対処を行う EDR（Endpoint Detection And Response）ソフトウェア等の利用や、主体の操作に対する常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ、ゼロトラストセキュリティ等）を用いて内部ネットワーク、外部ネットワーク問わずに対策を講じることも有効な手段として挙げられています。

以上の具体的な対策方法については、ガイドラインをご参照ください。

Q－２５　「小規模医療機関等で役割が自明の場合は、明確な規程を定めなくとも良い。」とあるが、小規模の基準は病床数や職員数で決められているのか。

Ａ　明確な基準はありませんが、自明とは「何ら説明を要しないこと」を指します。例えば、役割を果たすための有資格者が、その施設内に唯一人しか存在しない場合等です。そのような医療機関等では、明確な規程がなくとも説明責任を果たすことが可能であるか、検討する必要があります。

Q－２６　外部監査はどのような機関に依頼すべきか。

Ａ　医療機関等が少人数の従業者により運営されている等、内部監査の体制を構築できない場合には、第三者に監査を依頼することが考えられます。この「第三者」は、医療情報システムに関する知見を有していることが必要ですが、専門の監査機関等に限られるものではありません。

Q－２７　「個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること」とあるが、例えば外来やナースステーション等では、それらの措置は困難ではないか。

Ａ　外来やナースステーションでは患者や家族の入退がありますが、医療情報システムを導入していない場合にも行われているように、その事実をカルテ等に記録することにより、来訪を記録できます。

Q－２８　「パスワードの要件として、
a.英数字、記号を混在させた 13 文字以上の推定困難な文字列
b.英数字、記号を混在させた８文字以上の推定困難な文字列を定期的に変更させる（最長でも２ヶ月以内）」
として定めているが、どうしてなのか。

Ａ　パスワードの要件による安全性については、日々研究が進められています。近年では、定期的な変更を行うことで利用者が推定可能なパスワードを設定することで、むしろ脆弱になってしまうという報告（NIST SP800-63-3）もあります。

医療情報システムにおいては、患者情報を預かる医療従事者による職務上の安全確保という観点から、推定困難なパスワードを設定することが求められます。定期的な変更を行わず、前述の報告に記載されているような管理（※１）を適切に行うことで、最低限の安全性を確保できるパスワードとして、国内の他の基準等を参考にして、本ガイドラインでは、英数字、記号を混在させた 13 桁以上の文字列としています。

また、医療情報システムのシステム上の制約等で 13 文字以上の文字列を

設定できない又は適切な管理を行うことができない環境においては、推定困難なパスワードを、脆弱にならない形（※２）で定期的に変更させることにより、本ガイドラインでは、安全性を担保することとしています。この場合、英数字、記号を混在させた８文字以上の推定困難な文字列のパスワードでもよいとしております。

しかしながら、ID とパスワードによる認証では、安全性の確保に限度があります。前述の報告においても、患者情報のような個人情報へのアクセスは二要素以上の認証を組み合わせる認証方式（二要素認証）とすることが示されています。そのため、できるだけ早く二要素認証を導入することが求められます。本ガイドラインでは、令和９年度時点で稼働していることが想定される医療情報システムを、今後、導入または更新する場合、原則として二要素認証を採用することを求めています。導入または更新に際して、対象となる製品・サービスがベンダ等から提供されていないなどの理由で二要素認証対応が困難な場合にも、対象となる医療情報システムの利用に供する部屋の入室管理を個人ごとに特定できるようにする等の措置を講じて、全体として二要素認証に相当する安全性の確保を行う必要があります。

（※１）例えば、漏えいしたことのある及び推定可能な脆弱なパスワードを設定できない技術的な制約を課すことや、設定しようとするパスワードの強度が確認できること等の管理が挙げられています。（実装に関係される方は“Digital Identity Guidelines　から Authentication and Lifecycle Management”（NIST Special Publication 800-63B）
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf を参照してください）。

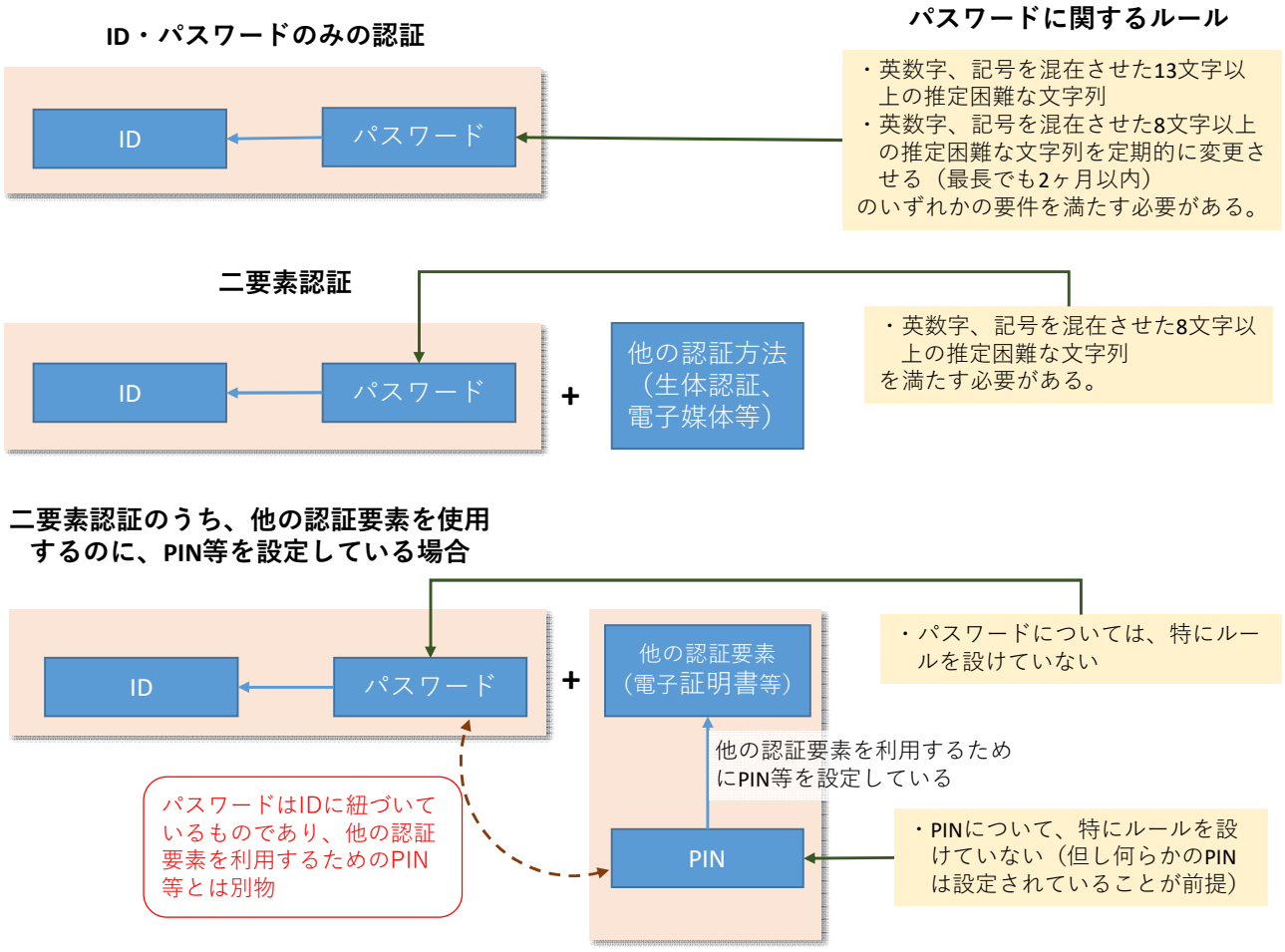
（※２）例えば、以前のパスワードから推定可能なパスワードといった解析のヒントを与えないような形が想定されます。

Ｑ－２９　「c.二要素以上の認証の場合、英数字、記号を混在させた８文字以上の推定困難な文字列。ただし他の認証要素として必要な電子証明書等の使用に PIN 等が設定されている場合には、この限りではない。」とあるが、具体的にはどのようなことを指しているのか。

Ａ　安全管理ガイドラインにおけるパスワードとは、例えば IC カードに格納されている電子証明書を使うために設定されている場合のＰＩＮではなく、ID（文字列）との組み合わせで認証する際のパスワード（文字列）を指しています。

二要素認証はＩＤ／パスワードのみの認証よりも安全性が高いことから、二要素認証におけるパスワードについては、同項ａ、ｂの要件（Ｑ－２８参照）とは異なり、８文字以上の推定困難な文字列であっても定期的な変更は求めないこととしています。

パスワード長については、原則として英数字、記号を混在させた８文字以上としていますが、例外として二要素認証のもう片方の認証要素を使う際に、ＰＩＮなどが設定されているなどの安全管理が施されている場合には、上記のパスワード長のルールは求めないこととしています。この理由は、ICカードに格納されている電子証明書等の認証要素（知識以外の要素）を使うために設定されている場合のＰＩＮは、ＩＤ／パスワード（知識）におけるＩＤに紐づくものではなく、厳密に言えばパスワードとは異なるためです。このようなケースでは利用者認証全体を勘案すると、ＩＤ／パスワードのほかに、ＩＣカード（所有）や指紋認証（生体）などの知識ではない認証要素、さらに追加の認証要素（知識）を利用するＰＩＮなどが設定されていることになるため、十分な安全性が確保されるものと評価されると考えられます。そのため、このような場合には、英数字、記号を混在させた８文字以上というパスワードの要件は求めないこととしています。具体的には下図の通りなります。



Q－３０　「確実に情報の破棄されたことを確認すること」とは立ち会いを前提としているのか。

A　立ち会いを前提とはしていません。破棄を行った証票を受け取る等、「6.6 人的安全対策　（2）事務取扱受託業者の監督及び守秘義務契約　C.最低限のガイドライン」の内容を遵守し、確実に確認していただければ問題ありません。

Q－３１　「情報機器を持ち出してよいのか、持ち出してはならないのかの切り分けを行うことが必要である。」とあるが、具体的にどのような基準で判断をすればよいか。

A　当該情報機器が医療情報を記録しているか否かで取扱いが異なります。

医療情報を記録している機器や媒体であれば、持ち出しには細心の注意が必要です。このような機器や媒体は、原則として持ち出すべきではないという基準にすべきです。その上で、やむを得ず持ち出す際には、情報機器を持ち出す必要性や漏えいのリスクを総合的に判断した上で、運用管理規程等に機器持ち出しの許諾ルールと判断基準を策定することが求められます。また、持ち出す機器については、6.9 章に示す適切な防護措置を施すことが必要です。

リモートサービス等により医療機関等の情報にアクセスできる機器の場合、医療情報を機器に記録していなくても、機器そのものの盗難や置き忘れが情報漏えいのリスクになります。このような場合、機器に対する防護措置に加え、リモートサービスそのものでの防護措置が必要であり、6.11 章に示された安全管理対策を実施していることが条件になります。

上記以外の情報機器については、機密情報の有無やその他の要件を考慮し、医療機関等における管理ルールを策定してください。

Q－３２　6.9 章における BYOD を行うに当たって、適切な技術的対策や運用による対策はどのようなものがあるか。

A　下記の対策等が挙げられます。

技術的対策としては、従業者のモバイル端末で、他のアプリケーション等からの影響を遮断しつつ、仮想デスクトップのような技術を活用して端末内で医療情報を取り扱うことを制限し、さらに個人でその設定を変更できないようにすること等が考えられます。この場合、OS レベルで業務利用領域（仮想デスクトップ）と個人利用領域を切り分け、管理領域を分離する必要があります。また、サービスや製品によっては十分な安全性が確保されない場合があるため、十分な知見を有する者が判断する必要があります。

さらに、上記の対策に加え、モバイルデバイスマネジメント（MDM）やモバイルアプリケーションマネジメント（MAM）等を施すことで、医療機関等が所有し、管理する端末と同等の安全性を確保するための、セキュリティ対策の徹底を図ることが期待されます。

また、運用による対策として、運用管理規程によって利用者による OS の設定変更（例えば、「設定」用のアプリケーションにより、医療情報システムへの接続に使用するアプリケーションに対して、他のアプリケーションが自動的にアクセスできるようにする等）を禁止し、かつ安全性の確認できないアプリケーションがモバイル端末にインストールされていないことを、管理者が定期的に確認すること等が想定されます。BYOD を行うに当たって、運

用管理規程に記載すべき事項の例を下記に示します。

【BYOD に係る運用管理規程への記載事項（例）】
BYOD を認める場合、管理者は下記を遵守すること。
・利用者に対し、端末や OS 等に応じて推奨されている適切な方法により、アプリケーションをインストールするよう指導すること。
・アプリケーション等の脆弱性に関する情報を収集し、利用者が脆弱性の明らかになったアプリケーションを使用していないか、定期的に確認すること。

Q－３３　災害等で電子システムが運用できない場合で、一時的に運用した紙データを後から電子システムに反映させることは、真正性の観点から問題にならないか（システムへの入力時のタイムスタンプが有効になるのではないか。）。

A　適切な安全管理が実施されていれば、問題ありません。「6.10　災害、サイバー攻撃等の非常時の対応」において要求事項が記載されているため、そちらを参照してください。

また、紙データを電子システムに反映させる際に、紙データをオリジナルとして保存する必要が生じると考えられます。オリジナルの紙データをスキャナ等により電子化して保存する場合は、「９　診療録等をスキャナ等により電子化して保存する場合について」を参照してください。

電子カルテ等に転記した場合、転記した情報で診療等を実施することに問題はありません。ただし、オリジナルとしての紙若しくはスキャナ等で電子化したデータは、別途適切な安全管理を実施した上で、定められた期間保存する必要があります。

Q－３４　6.10 章 C 項 4⑷において、「重要なファイルは数世代バックアップを複数の方式で取得し、」とあるが、外部からの攻撃を受けた場合の復旧のための対応としては、どのような点を考慮して、バックアップを取得する必要があるか。

A　バックアップ取得のポリシーは、医療の社会的な影響度を鑑みて、医療機関等における診療業務の継続性を確保するため、できる限り診療に影響に及ぼさないよう、計画を立てることが求められます。この部分は一般企業にお

けるバックアップに対する考え方との大きな違いになります。
　但し具体的なバックアップ取得の計画については、取扱うデータの利用頻度やシステムが停止した場合に復元すべき時点、システムの特性などを考慮して、総合的に決定されるため、一意に決まるわけではありません。
　例えばバックアップの取得範囲として、通常、フルバックアップ、差分バックアップ、増分バックアップなどがあり、適切に組み合わせて、対応することになります。
　そのうえでさらに具体的な例として、日次で差分バックアップ、週次でフルバックアップを行う場合、前々週以前のフルバックアップ及びその週以前の日時の差分バックアップは、ネットワークから切り離した記録媒体で保管すること（磁気テープ、DVD、Blu-Ray 等）あるいは論理的に書き込み禁止（磁気ディスク等）の状態にする等の対策が必要となります。
　最近ではクラウドサービスを利用したバックアップを行うことも考えられます。例えば、原本データ以外にクラウド上でバックアップを取得する場合、バックアップデータを追記できない設定としたり、複数のバックアップデータを取得したりするなどの方式で、複数方式によるバックアップを行うことが想定されます。
　また電子カルテ、医事システム、LIS、RIS（PACS 含む）等のサブシステムがそれぞれデータベースを持つ場合、それぞれについてシステム特性やデータの影響度を鑑みて、バックアップ取得の計画を策定することになります。
　具体的な例としては、電子カルテ、LIS 等保存データがあまり大きくないサブシステムについては、日次でバックアップを確保し、電子カルテは５世代、その他のシステムは３世代保存するなどにより、前週までのデータを回復することが想定されます。この場合、ランサムウェア等の攻撃への対策という観点から、電子カルテで３世代以降のバックアップデータについては、ネットワーク的あるいは論理的に書き込み禁止属性とし、その他のシステムは３世代目をネットワーク的あるいは論理的に書き込み禁止とするなどが求められます。
　一方、PACS を含む RIS のような大量のデータを扱う場合はバックアップそのものが困難な場合もありえます。この場合には、サイバーセキュリティを考慮すると、確定されたデータについては書き込み禁止に設定するべきです。そのうえで、運用上可能であれば、例えばキー画像の指定がされた画像データ等は電子カルテと同様の対策するなどにより、医療の継続性の確保において極めて有用な対応になると考えられます。
　バックアップ計画の策定に際しては、利用する医療情報システムやサービスを提供する事業者からの情報提供等を踏まえて検討することが重要です。例えば「「製造業者/サービス事業者による医療情報セキュリティ開示書」ガ

イド」[3]では、「医療機関等には、情報を保存する場所や、その場所ごとの保存可能容量、リスク、レスポンス、バックアップ頻度、バックアップ方法等を運用管理規程にまとめ、関係者に周知することが求められます。」（P24）とし、事業者によるバックアップに関する情報提供の有無が確認できることとなっています。事業者から情報提供されている場合には、その内容などを参考に、計画の策定を行うことが考えられます。また医療機関等が自らシステム構築を行う場合には、「非機能要求グレード 2018」（独立行政法人情報処理推進機構）などを参考に、バックアップ計画を策定するなども一案です。

Q－３５　セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）とは、具体的にどのような事象を指すものか。

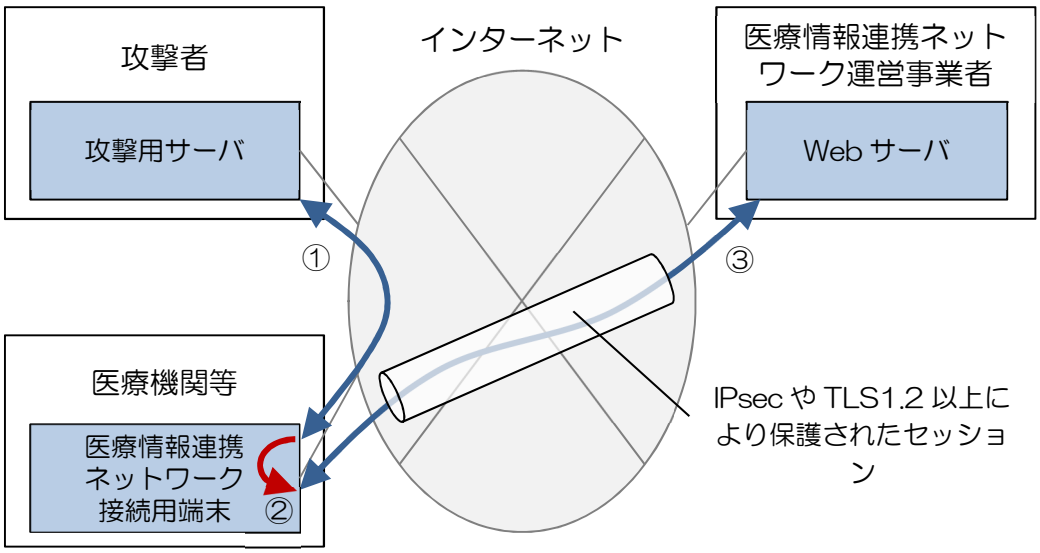
Ａ　例えば、下図のように、医療情報連携ネットワークの Web サーバへのアクセス等のために、医療機関等の専用端末がソフトウェア型の IPsec や TLS1.2 以上によりオープンネットワークに接続している場合、攻撃者は開放された当該端末のポートを標的として、何らかの攻撃（典型的には標的型メール攻撃等）を試みることが想定されます（①）。

　この攻撃により、当該専用端末が遠隔操作型のマルウェア等に感染すると、攻撃者は本人になりすまして医療情報連携ネットワークの Web サーバとのセッションの立上げを試みることが可能になります（②）。セッションの立上げに成功すると、外観上は正規の権限によるアクセスが発生することになり、IPsec や TLS1.2 以上により適切に暗号化していても、攻撃者は医療情報連携ネットワークの Web サーバにアクセスできるようになります（③）。

　ガイドラインでは、この一連の攻撃を「セッション間の回り込み」と称しています。対策として、適切な経路設定を実施することに加え、医療情報連携ネットワークへのアクセスに当たって、二要素認証により利用者の識別・認証を行うことで、遠隔操作を防ぐこと等が考えられます。

[3] 一般社団法人保健医療福祉情報システム工業会、一般社団法人日本画像医療システム工業会医用画像システム部会セキュリティ委員会

【セッション間の回り込み　イメージ図】



Q－３６　「従業者による外部からのアクセスに関する考え方」に、「仮想デスクトップを導入した際の運用等の要件にも相当な厳しさが要求される」とあるが、どの程度か。

Ａ　従業者による外部からのアクセスで問題になることは、利用するＰＣや通信経路等の状態、及び周囲から盗み見されるおそれがある等、従業者の作業環境が管理できないことです。例えば、ＰＣにキーボードロガーのような不正ソフトウェアがインストールされているリスクや、空港や喫茶店等でアクセスすれば周囲の人に覗かれるリスクがあります。

仮想デスクトップは、不正ソフトウェアの作用を避け、ＰＣ上に情報が残留することを防ぐ目的で使用されます。また、通信経路の安全性を確保するため、ＶＰＮの成立と連動して稼働することが望まれます。運用としては、周囲の環境に十分注意して盗み見を防止するとともに、過去のログイン時間の確認を確実に行うこと等を通じて、不正アクセスの検出に努める必要があります。

Q－３７　6.11 章の C.10 に「 SSL-VPN は利用する具体的な方法によっては偽サーバへの対策が不十分なものが含まれるため、使用する場合には適切な手法の選択及び必要な対策を行うこと」とあるが、具体的

にはどのように利用するのか。

Ａ　安全管理ガイドラインでは、偽サーバへの対策が不十分なものが多いため、医療情報システムでは原則として使用するべきではないとしています。しかしSSL-VPNについてもクライアント型と呼ばれるものについては、「専用のクライアントソフトがインストールされた端末との間でのみアクセスする。つまり、誤って偽サーバに接続することがなく、また内部サーバにアクセスできる端末も厳格に制限できるため、端末に IPsec-VPN ソフトをインストールして構成するモバイル型の IPsec-VPN に近い形での運用形態」が可能とされています（「TLS 暗号設定ガイドライン 3.01 版」IPA）。

従って、SSL-VPNを利用する場合には、6.11 章の C.10 に記載されているクライアント証明書を利用した TLS クライアント認証や「高セキュリティ型」に準じた適切な設定を行った上で例外的にクライアント型の SSL-VPN などの利用によることが考えられます。

Ｑ－３８　「ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路を設定すること。安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティターゲット又はそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。」とあるが、

① ソフトウェアは、安全性の確認対象から外れるのか。

② 安全性を確認するための方法は他にないか。

Ａ

① ここでいうソフトウェアが「ルータ等のネットワーク機器の機能をソフトウェアで実現しているもの」を指すのであれば、その当該ソフトウェアに対して安全性が確認できる必要があります。「ルータ等のネットワーク機器」を「当該ソフトウェア」に読み替えてご対応ください。

② ISO/IEC 15408 で認証された機器を導入することが必須ではありません。このガイドラインが求める安全対策のための要求事項を、導入を検討している機器ベンダに示して、回答を求めてください。満足する回答が得られれば、安全性が確認された機器と判断していただいて結構です。

Q－３９　「電気通信事業者やシステムインテグレータ、運用を受託する事業者、遠隔保守を行う機器保守会社等の多くの組織が関連する。そのため、次に掲げる事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。」とあるが、契約書の記載方法を教えてほしい。

Ａ　6.11 章「C.最低限のガイドライン　6.」に掲げている事項に関し、個別に責任範囲及び共同対応範囲を定めて、誰が何をどのタイミングで行うかを文書化してください。

また、通信サービスを提供する事業者等に対しては、SLA（Service Level Agreement）を確認し、SLA に記載されていない若しくは不足する部分があれば、その部分について SLA の修正を要請する又は個別契約を結ぶことで対応してください。

Q－４０　6.12 章 C 項の 1⑵⑹の２つ目の「・」の最初の「-」にある「医療機関等の管理者」とは、具体的には組織単位で考えればよいか。

Ａ　本ガイドラインにおける医療機関等とは「病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等」を指します。従ってここでも医療機関等ごとに管理者を設置することを想定しています。例えば、同一法人に複数の病院や診療所、薬局等が属している場合でも、それぞれの病院や診療所、薬局等の単位で管理者を設置することになります。

Q－４１タイムスタンプはパソコンの時間と同じでよいか。

Ａ　タイムスタンプは電子署名を含む文書全体の真正性等を担保するために必要なものであることから、このガイドラインでは「時刻認証業務の認定に関する規程」（令和３年４月１日、総務省告示第 146 号）に基づき認定された事業者（認定事業者）が提供するものを利用することを求めています。※

※ 一般財団法人日本データ通信協会が認定した時刻認証事業者（以下「認定時刻認証事業者」という。）については、令和４年以降、上記の国による認定制度に順次移行する予定であることから、当面の間、認定時刻認証事業者によるものを使用しても差し支えありません。

Q－４２　通常閉じたネットワークで構築することが多い医療機関等において、一枚一枚の文書にリアルタイムにタイムスタンプを付与することは、実装が困難ではないか。

Ａ　「6.12　法令で定められた記名・押印を電子署名で行うことについて」は、診療情報提供書や診断書等の法令で記名・押印することが定められた文書等を対象としています。これら以外の文書等に一枚一枚タイムスタンプを付加することは必須ではありません。

しかしながら複数のスキャン画像ファイルなどにまとめてタイムスタンプを付す場合、方式によっては個々のファイルを個別に検証することができなくなるので留意が必要です。例えば、複数ファイルを ZIP ファイルに格納してタイムスタンプを付与した場合、タイムスタンプの検証時に ZIP ファイル全体を読み込む必要があり、ファイル個別に検証することができません。係争時等の外部提出を想定した場合に、関係のないファイルも提出する必要があるため適切な方法とはいえません。

そのため個別のファイルごとにタイムスタンプを検証することができる標準技術を使用すれば、適切にタイムスタンプを付すことができます。標準技術の例として、個々のファイルのハッシュ値を束ねて階層化した上で、頂点のハッシュにタイムスタンプを付す ERS（Evidence Record System）等があります。

なお、タイムスタンプを付与するにはセキュアなタイムスタンプ環境を構築する必要があります。

「7　電子保存の要求事項について」関係

Q－４３　部門系で発生する記録等は、ガイドラインでいう診療録等としての適用を受けるのか。

例えば、エコー検査の紙画像や心電図の紙波形結果等、院内で発生した文書（ワープロやシステム出力）で、かつ手書き情報の付記のないものについては、スキャニングした電子化情報を原本として、元の紙を廃棄してよいか。

※　スキャニングする際、どの患者の結果で、誰が、いつ記録したか、は登録することを前提とする。

※　紹介状や同意書等、外部からの文書や押印して初めて効力が発生する文書は、紙を原本として残すのが原則である。

上記の場合、診療録等として確定することになるのは、どの行為の時点になるのか。

スキャニング時の作業責任者と情報作成管理者は、どのようになるのか。

また、情報作成管理者は、有資格者等である必要があるのか。

手書きの付記等がある場合は、どのように行えばよいのか。

Ａ　診断の根拠となる記録や診療方針に影響を与える記録等は、定められた期間保存する必要があります。紙等の物理媒体の保存義務がある記録をスキャナ等により電子化して保存する場合は、「９　診療録等をスキャナ等により電子化して保存する場合について」を参照してください。

確定については、紙等の記録が作成された時点で記録は確定しており、確定された記録を電子化しているため、「９　診療録等をスキャナ等により電子化して保存する場合について」に規定されるように、電子化された情報を保存義務の対象として扱うことができます。

作業責任者と情報作成管理者は運用管理規程等で定め、適正に運営されていることを監査すること等が求められますが、有資格者である必要はありません。

Q－４４　電子カルテを導入した場合、それまでの旧カルテ（紙カルテ）について保存義務があるか。あるとすれば何年か。

Ａ　紙の診療録の法定保存年限は医師法で一連の診療の終了後５年とされてい

ます。ただし、電子カルテの導入により、以前の紙の診療録がスキャナ等で適切に電子化されており、管理責任者によって保存義務の対象が電子化された診療録であると認められていれば、紙の診療録に法定上の保存義務はありません。このような処理を行わない場合は、法定の保存義務があります。

なお、情報の真正性、保存性の確保の観点から、スキャナ等で電子化して運用する場合でも、元の媒体である紙の診療録を併せて保存することは有効であり、法定期限に限らず保存することが望ましいです。ただし、この場合も電子化及び保存に関しては、「９　診療録等をスキャナ等により電子化して保存する場合について」等を参照の上、適切に実施する必要があります。

Ｑ－４５　真正性の確保について、記載されている情報と確定者には具体的にどのような組み合わせがあるか。

Ａ　情報と確定者の組み合わせとしては下記のような例があります。

例 1）　医師が患者の診察時にカルテに所見を記述する。

情報　：所見

確定者　：実際に診察を行った医師

例 2）　看護師が医師の指示に基づく処置を行った際に、実施状況を看護記録に記述する。

情報　：処置実施記録

確定者　：実際に処置を行った看護師

例 3）　読影担当医が放射線画像の読影レポートを作成する。

情報　：読影レポート

確定者　：読影を行った放射線科医師

例 4）　検査技師が検査ラインから出力された検査結果のバリデーションを実施し、システムに取り込む。

情報　：検査結果

確定者　：バリデーションと取り込み操作を行った検査技師

例 5）　夜間等で当直医が主担当医の電話での指示により、指定された薬剤のオーダ入力を行った。

情報　：投薬指示

確定者　：実際にオーダを実施した当直医

Ｑ－４６　7.1 章 C 項において、「確定者が何らかの理由で確定操作ができない場合における記録の確定の責任の所在を明確にすること。例えば、

医療情報システム安全管理責任者が記録の確定を実施する等のルールを運用管理規程に定めること」とあるが、具体的にどのような場合を指すか。

Ａ　例えば、在宅で治療を行っている患者の様態が急変した等、緊急で対応すべき事由が発生したため、確定操作を行う時間的余裕もなく、担当医が外出せざるを得なくなった等の事例が考えられます。

Ｑ－４７　代行入力を行う場合、代行を許可した証拠はどのように残しておけばいいのか。

Ａ　代行入力を実施する場合には、必ず入力を実施する個人ごとに ID を発行し、代行入力を行う者はその ID でシステムにアクセスしなければなりません。その際、入力者のログ、あるいは作業報告等の台帳を作成し、記録を残す必要があります。

また、誰の意思決定に基づいて代行入力を実施したかが説明できるように、上記の内容を含めた代行入力に関する運用管理規程等の策定が必要です。

Ｑ－４８　記録を確定する方法として、①入力者が情報を入力画面を見ながら入力して記録する場合、②外部機器等から確定されていない情報を取り込み記録する場合、③外部システムで確定された情報を取り込み記録する場合が考えられるが、それぞれどのように対応すべきか。

Ａ　確定操作は、文書の責任者が誰かを明らかにし、操作の時点で対象とする文書の記述に誤入力や改ざん等がないことを保証し、記載に対して責任を持つという意味合いがあります。そのため、上記①～③の対応について下記のように考えられます。

①「入力者が情報を入力画面を見ながら入力し記録する場合」

この場合には、確定するという操作を行うことで、内容を確定者が保証することになります。「確定者が」としたのは、文書の入力を確定者が自ら行う場合や代行入力による場合があるからです。いずれの場合も、運用管理規程等によって決められた確定者が確定したということになります。また、処理としては署名を施す等になります。

代行入力の場合には、確定者が必ず確認を行った上で、確定を実施しな

ければなりません。

②「外部機器等から確定されていない情報を取り込み記録する場合」

この場合には入力者が、記述の改ざんや誤入力等がないことを確認した上で、スキャナ等による読み込みを行い、誰の記録であるかを関連付けして、①の確定操作を行うことになります。

③「外部システムで確定された情報を取り込み記録する場合」

改めて受け取り側で確定操作を行う必要はありませんが、外部システムで確定されていることを確認することが必要です。ただし、確定された情報しか取り込まれないようにシステムが構築されている場合、その限りではありません。

Q－４９　X 線 CT の検査で、オリジナルの画像のほかに、オリジナル画像から生成した３D画像も使って診断している。

電子保存を行う際に、オリジナル画像さえ保存しておけば、診断に使用した３D画像は消去してしまっても構わないか。

3D 画像作成時のパラメータは保存されていないため、診断の際に生成した３D画像を完全に再現することが難しい状況である。

A　オリジナル画像から当該画像を生成することが原理的に可能であれば、直接診療に使用した処理画像データを保存しておく必要はありません。しかし、この例では、３D画像作成のパラメータがないと診断に用いた画像を完全に再現することが困難であるということなので、3D 画像を消去することはできません。

Q－５０　外部の医療機関等から持ち込まれた X 線写真（コピー）や画像データを当院での診療に用いた場合、保存義務は生じるのか。

A　原本の保存義務は元の医療機関等にありますが、持ち込まれた診療情報を診療に利用した場合は、当該医療機関等においても保存義務が発生します。

Q－５１　3D 画像処理を行った場合、処理を行う元となった画像は保存しなければならないか。

A　3D 画像処理を行う元となった画像を、3D を作成することのみに用い、

診断に用いないならば保存する必要はありません。診断用に作成した 3D 画像は保存する必要があります。

Q－５２　確定保存された画像に関し、診断や患者説明のために一時的に医師が表示方法（濃度の変更、拡大など）のみを修正した場合、この画像を保存する必要があるか。

Ａ　濃度の変更、拡大といった程度の処理ならば、改めて保存する必要はありません。

Q－５３　検像において、検像前の画像情報、検像後の画像情報のいずれを保存対象とすべきか。

Ａ　「検像」についての確かな定義はないため、ここでは医師の診断や読影のために、診療放射線技師等が画像の確定前に当該画像を確認し、必要に応じて画像の付帯情報の修正や不必要な画像の削除を行うことを指すものとします。保存義務の対象とすべき画像については、検像の後に診断に用いるのであり、検像後の画像を対象とすべきと考えられます。ただし、検像において情報の修正・削除といった行為により、照射記録と検像の後の画像情報が一致しない等のことが生じる場合には、修正履歴を保存しておく等、所定の措置が必要となります。また、これらの行為に対する責任の所在を組織として説明できるようにしておく必要があります。

Q－５４　画像の確定に当たっては明示的な確定操作が必要か。

Ａ　必ずしも必要ではありません。例えば、①PACS が受信した時点、②PACS で受信してから一定時間経過した時点、③PACS で受信してから一定時刻を過ぎた時点をもって確定とすること等が考えられます。これらについては、各医療機関等において、運用管理規程に明記することが必要です。

Q－５５　事前の確認時と状況が変わり、請負事業者が倒産する等してソフトウェアの保証がなくなった場合、見読性は確保されていないことになるのか。

Ａ　倒産ではなく、請負事業者がソフトウェア事業を廃止する場合は、見読性を確保する条項等を契約書に明記することで、見読性を確保できます。
　しかし、倒産の場合、使用継続は保証されるものの、長期の見読性は保証されないこととなり、使用者がこれを担保する必要があります。診療等に差し支えない期間内に見読性が保証される対策を講じなければならず、この対策を容易にするためにも標準化や相互運用性の確保は重要です。

Ｑ－５６　「大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップ」とあるが、「遠隔地」の定義はあるのか。

Ａ　具体的な定義はありませんが、当該医療機関等が地震等の大災害に見舞われた場合でも、それらの被害を受けず、安全に保存できると考えられる地域と考えられます。

Ｑ－５７　「ネットワークを通じて外部に保存する場合」に「緊急に必要になることが予測される診療録等は、内部に保存するか、外部に保存しているものの複製又は同等の内容の情報を医療機関等の内部に保持する」とあるが、具体的にどの程度か。

Ａ　各医療機関等の機能により判断すべきですが、診療録等の参照が迅速に行えないことで、患者の生命や身体に重大な影響を及ぼすおそれがあることが想定されるものが対象となります。例えば、これから手術を行う方や入院されている方の診療録等が想定されます。通常１週間程度のデータ、あるいは前回の診療データも目安になります。

Ｑ－５８　「診療録等のデータについて、標準形式が存在する項目は標準形式で、標準項目が存在しない項目は変換が容易なデータ形式で、それぞれ出力及び入力できる機能を備えること」とあるが、標準形式は正式に定められたものがあるのか。

Ａ　「５　情報の相互運用性と標準化について」に、現時点での標準形式が挙げられているため、参照してください。なお、今後も追加や更新がされるため、適宜確認してください。

Ｑ－５９　医療情報を電子化するに当たって定められた要件は何か。

Ａ　「Ｑ－２３」のＡを参照してください。

「8　診療録及び診療諸記録を外部に保存する際の基準」関係

Ｑ－６０　掲示以外の周知方法はどのようなものがあるか。

Ａ　院内掲示以外の周知方法としては、パンフレットの配布、問診表への記載、医師・看護師等による口頭説明等があります。さらに、インターネットホームページでの公表を加えることもできます。

Ｑ－６１　電子化された診療情報は外部保存できるか。その際の要件は何か。

Ａ　電子媒体による外部保存をネットワークを通じて行う場合は「8.1　電子媒体による外部保存をネットワークを通じて行う場合」に、電子媒体による外部保存を可搬媒体を用いて行う場合は付則１に、それぞれ要件が記載されているため、そちらを参照してください。なお、いずれの場合においても別冊「旧８.４　外部保存全般の留意事項について」に留意する必要があります。

Ｑ－６２　地域連携のための医療情報システムとして、医療情報の所在だけを管理するレジストリと、各医療機関等が共有のために確保するリポジトリを設置する形態をとっている。利用者は、レジストリにアクセスして所在を知り、リポジトリにアクセスして実際の情報を利用する方式をとることができる（IHE　XDS 統合プロファイル※）。この場合、各医療機関等は互いに保管された医療情報を共有する形となるので、共同利用という形と考えてよいか。
　また、レジストリは民間事業者等のデータセンターを利用するこ

とが適当と考えられるが、各医療機関等はデータセンターに所在情報の管理を委託してもよいか。
※https://www.ihe.net/

Ａ　診療情報を「共同利用」するためには、個人データを特定の者との間で共同して利用することを明らかにし、利用する個人データ項目、利用者の範囲、利用目的、個人データの管理責任の所在等を、あらかじめ本人に通知等している必要があります（詳細は「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」を参照してください。）。本ケースの場合は、これらの要件が不明確ですので、共同利用の要件を満たしていない可能性があります。共同利用の要件を満たしてない場合、他の施設での診療情報の利用は第三者提供に当たります。また、レジストリについて医療機関等以外の外部の事業者のデータセンターを利用する際には、医療情報を外部保存する場合と同等の要件を満足する必要があります。

Ｑ－６３　医療情報を共同利用する場合、どのような留意事項があるか。

共同利用は、個人データの第三者提供の例外として個人情報保護法上認められている個人データの利用形態です（個人情報保護法第 27 条第 5 項第 3 号）。これは、形式的には個人データを直接の提供先とは別の組織が利用するものの、本人からみて、直接個人データを提供した相手先と一体的な利用であると合理的に考えられるため、共同利用する者は第三者には含まれないという趣旨に基づくものです。例えば地域医療連携や共同研究などの場合に、このような利用が認められる場合があります。共同利用は無限定になされると、本人（患者等）の利益を損なうことから、共同利用者の範囲や利用目的などが、「本人が通常予期し得ると客観的に認められる範囲内である必要」があります（「個人情報の保護に関する法律についてのガイドライン（通則編）」3-6-3（個人情報保護委員会））。共同利用の考え方については、上記ガイドラインを参照ください）。

なお共同利用については、令和２年改正法により、本人への通知等の義務が強化され、共同利用の事実、共同利用の対象となるデータ項目、利用者の範囲、利用目的、管理責任者の指名等の通知等のほか、管理責任者の住所、法人代表者の氏名も併せて本人への通知等の対象となりました。

Q－６４　クラウド型の電子カルテサービスを行う業者に認定制度のようなものはあるのか。もしなければ、業者を選定する際に３省のガイドライン※に準拠していることは、どうやって確認すればよいのか。

Ａ　認定制度は現在のところ存在しません。なお、厚生労働省のガイドラインは、サービス提供業者ではなく、サービスを委託する医療機関等が遵守すべきものです。

サービス業者の選定に当たっては、「「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」に準拠している旨」をサービス業者に確認させるとともに、契約を結ぶ際に、その旨を条項に盛り込んでおくとよいでしょう。

また、サービスを委託する医療機関は、当該サービスを利用した運用形態が、厚生労働省のガイドラインに準拠していることを、自ら確認してください。

※ ３省のガイドラインとは以下のガイドラインを指します。
医療情報システムの安全管理に関するガイドライン
医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（総務省、経済産業省）

Q－６５　もし、委託したクラウド型の電子カルテサービス業者から自院の患者に関するデータが漏えいした場合、自院にはどのような責任が問われるのか。

Ａ　本ガイドラインの「4.2.1　委託における責任分界」の記述が適用されます。

管理責任はあくまでも医療機関等の責任者にあり、万一事故が起きた際には、受託する業者と連携しながら本ガイドライン「4.1」項の「説明責任」と「善後策を講ずる責任」を果たす必要があります。

Q－６６　クラウド型の電子カルテサービスを行う場合、利用者によるトランザクションごとに電子署名が必須となるのか。

Ａ　電子署名の付与に関する記述への対応として、個々のトランザクションを

「ファイル」と考えれば、各々の情報単位で電子署名が必要になると解釈できないことはありません。しかし、ここではそれほど厳密な解釈を適用せず、トランザクション単位での電子署名の付与は不要だと考えられます。

本質問にある電子署名の付与には、２つの目的があると考えられます。１つは外部のネットワークを経由する際のメッセージの真正性の担保、もう１つはサービス側で情報を保存する際の真正性の担保（改ざん防止等の完全性の観点、否認防止の観点等）です。

これらを同時に満足するための技術的手法として、電子署名の付与は有効な方法です。しかし、これを個々のトランザクション・メッセージに適用することは必須ではありません。例えば、通信経路上の改ざん防止には、メッセージに電子署名を付与しないでも、TLS 等の適用で十分な場合があります。また、メッセージを保存する際に逐次電子署名を付与しなくても、それよりも大括りな情報単位（例えば一日単位）で電子署名を付与すること、あるいは本ガイドラインに例示された他の技術的手法・運用方法を適用することも可能です。

「9　診療録等をスキャナ等により電子化して保存する場合について」関係

Ｑ－６７　9.1 章のＢ項にある「また、スキャニングにより、保存できない有用な情報」とは、どのようなものがあるか。

Ａ　現在のスキャナの機能は向上しており、高い解像度での読み取りや筆圧などを記録できるものもあります。一方、紙媒体においては、例えば、患者が疾患・症状から書面作成時に用紙をペン先で突き破ってしまったり、用紙の固定がうまくできず、不規則な折れ目（しわ）が付くこともあります。

このような変化はスキャナで必ずしも正確に記録できないことがあるため、このような場合の記録を電子的に行う際は、スキャナで電子化するのではなく、適切に動画撮影をする方が正確な記録となる可能性があります。

このようにスキャナで直接記録される文字情報等以外に、紙媒体の物理的な状態などの有用な情報があることについて、示したものです。

Q－６８　診療の用途に差し支えない精度の基準はあるか。

Ａ　画一的な基準はありません。手書き文書、ワープロ印刷文書、インスタント写真等、対象ごとに診断等の診療目的の利用に十分な精度を満たしていることをあらかじめ確認した上で、運用管理規程等で定めてください。

なお、第３版までは 300dpi、RGB 各８ビット以上としていましたが、一般に安価のスキャナでもこれ以上の性能を持つものが大多数を占めるために、記載を改めたものです。不用意に精度を下げることを推奨しているものではありません。

Q－６９　汎用性が高く、可視化するソフトウェアに困らない形式にはどのようなものがあるのか。

Ａ　医療情報には様々な形態の情報があり、画像、図形、波形、テキスト、数値、グラフ等の形式のデータから構成されています。これらのデータを一様に見ようとするならば、画像化することが、おそらく最も汎用性の高い可視化手段になるでしょう。デジタル情報を画像化するには、PDF（Portable Document Format）が最も一般的なだと考えられます。紙やフィルムの形で存在する場合には、スキャナで画像化することで可視化できますが、この場合には JPEG（Joint Photographic Experts Group）、PNG（Portable Network Graphics）等の形式を利用することができます。

これらのフォーマットは、PC に組み込まれていたり、ダウンロードすることで容易に取得できるソフトウェアによって可視化することができます。

Q－７０
① 診療録等をスキャナで電子化した場合、原本の取扱いはどのようにすべきか。
② 電子化された場合、法定保存年限を経過した文書も保存すべきと考えるべきか。

Ａ　「9.1　共通の要件」の記載に従って電子化し、電子化されたものを保存義務のある対象とする場合は、スキャンされた原本は個人情報保護の観点に注意して廃棄しても構いません。しかし、電子化した上で、元の媒体も保存することは真正性・保存性の確保の観点からきわめて有効であり、破棄を義

務付けるものではありません。また、法定保存年限を経過した文書の保存期限は、各医療機関等で規定することとなります。

Q－７１　「スキャナによる読み取りの際の責任を明確にするため、作業責任者（実施者又は情報作成管理者）が電子署名法に適合した電子署名・タイムスタンプ等を遅滞なく行うこと。」とあるが、これは取り込み責任者を明確にすることか。

Ａ　取り込み責任者を明確にする目的だけでなく、改ざんやなりすましを防止するために、また、作業内容の正確性についての説明責任を果たすために実施するものです。

Q－７２　「情報が作成されてから又は情報を入手してから一定期間以内にスキャンを行うこと。」とあるが、一定期間以内とはどれ位をいうか。
　外来診療の場合、１日の診療が終わった後にまとめて行う等の運用でもよいか。

Ａ　原則は１日以内です。ただし、深夜に来院し、次の日が休診である場合等は営業日として１日以内となります。

Q－７３　「「電子化した紙の調剤済み処方箋」を修正する場合、「『元の』電子化した紙の調剤済み処方箋」を電子的に修正し、「『修正後の』電子化した紙の調剤済み処方箋」に対して薬剤師の電子署名が必須となる。電子的に修正する際には、「『元の』電子化した紙の調剤済み処方箋」の電子署名の検証が正しく行われる形で修正すること」とあるが、電子保存した内容を再度プリントアウトして、訂正後に再度電子化して保存するといった運用でもよいか。

Ａ　調剤済み処方箋をスキャナ等により電子化し、電子化した情報を原本とした後に修正を行う場合、真正性の確保の観点から、過去の電子署名の検証が可能な状態を維持する形で電子的に修正し、薬剤師の電子署名を付す必要があります。
　そのため、プリントアウトしたものに訂正を行い、再度スキャナ等により電子化して保存することは、真正性の確保の観点から適切ではないと考えま

す。
　スキャナ等による電子化は、９.１章に規定されているように、医療機関等において運用管理規程を適切に定めて実施されるものです。
　例えば、事後修正が生じる可能性が十分低くなってから、スキャン等により電子保存する、又はスキャニングした紙の調剤済み処方箋を一定期間バックアップとして保存すること等が考えられます。このような対応を講じることで、当該処方箋に修正の必要が生じた際に、スキャン等により電子化した情報を破棄した上で、その紙媒体を原本として修正を行い、改めてスキャン等により電子保存することができます。

Ｑ－７４　「緊急に閲覧が必要になったときに迅速に対応できるよう、保存している紙媒体等の検索性も必要に応じて維持すること。」とあるが、どのようなケースで、どれくらいの対応時間内で行う必要があるのか。

Ａ　運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保存を行う場合、電子化した情報はあくまでも参照情報です。
　緊急時とは、例えばシステムダウン等が想定できます。また、一般に「診療のために直ちに特定の診療情報が必要な場合」とは継続して診療を行っている場合であり、患者の診療情報が緊急に必要になることが予測されるときは、診療に差し支えない範囲で原本である紙媒体を閲覧可能な状態にしておくことが必要です。

Ｑ－７５　医療情報を電子化するに当たって定められた要件は何か。

Ａ　「Ｑ－２３」のＡを参照してください。

Ｑ－７６　災害等で電子システムが運用できない場合で、一時的に運用した紙データを後から電子システムに反映させることは真正性の観点から問題にならないか（システムへの入力時のタイムスタンプが有効になるのではないか。）。

Ａ　「Ｑ－３３」のＡを参照してください。

Ｑ－７７　部門系で発生する記録等は、ガイドラインでいう診療録等としての適用を受けるのか。

例えば、エコー検査の紙画像や心電図の紙波形結果等、院内で発生した文書（ワープロやシステム出力）で、かつ手書き情報の付記のないものについては、スキャニングして電子化情報を原本として、元の紙を廃棄してよいか。

※　スキャニングする際、どの患者の結果で、誰が、いつ記録したか、は登録することを前提とする。

※　紹介状や同意書等、外部からの文書や押印して初めて効力が発生する文書は、紙を原本として残すのが原則である。

上記の場合、診療録等として確定することになるのは、どの行為の時点になるのか。

スキャニング時の作業責任者と情報作成管理者は、どのようになるのか。

また、情報作成管理者は、有資格者等である必要があるのか。

手書きの付記等がある場合は、どのように行えばよいのか。

Ａ　「Ｑ－４３」のＡを参照してください。

Ｑ－７８　掲示以外の周知方法はどのようなものがあるか。

Ａ　「Ｑ－６０」のＡを参照してください。

「10　運用管理について」関係

Ｑ－７９　医療機関等がこのガイドラインに基づき、診療録等の電子保存に係る運用管理規程を作成し、その規定に沿って運用している場合、「C. 最低限のガイドライン」を満足していない項目があった場合、問題となるのか。

Ａ　たとえ手段が異なっていても、ガイドラインの趣旨を踏まえて、同様の効

果を発揮するように実施することが求められます。「C.最低限のガイドライン」を満足していない状態で何らかの問題が発生した場合は、安全管理上の必要な措置を行っていないとみなされる可能性があります。少なくとも、「C.最低限のガイドライン」に沿った対応を行っていないことについて、理由の説明が求められます。

「付則」関係

Q－８０　掲示以外の周知方法はどのようなものがあるか。

Ａ　「Q－６０」のＡを参照してください。

「付表」関係

Q－８１　医療情報システム導入に際して規程等を作成したいが、どのようなものが望ましいのか。

Ａ　個人情報保護方針については、「6.1　方針の制定と公表」において個人情報保護対策の制定について説明があります。また、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」では、「Ⅰ　6．医療・介護関係事業者が行う措置の透明性の確保と対外的明確化」に要求事項が記載されているため、参照してください。

運用管理規程については、「6.3　組織的安全管理対策（体制・運用管理規程）」において、運用管理規程についての説明があります。運用管理規程については、付表に作成例が掲載されているため、参考にしてください。

Q－８２　付表に記載されている文例は、全くこのとおりにする必要はないということか。

Ａ　必要ありません。文面は、医療機関等の実情に応じて変更して下さい。